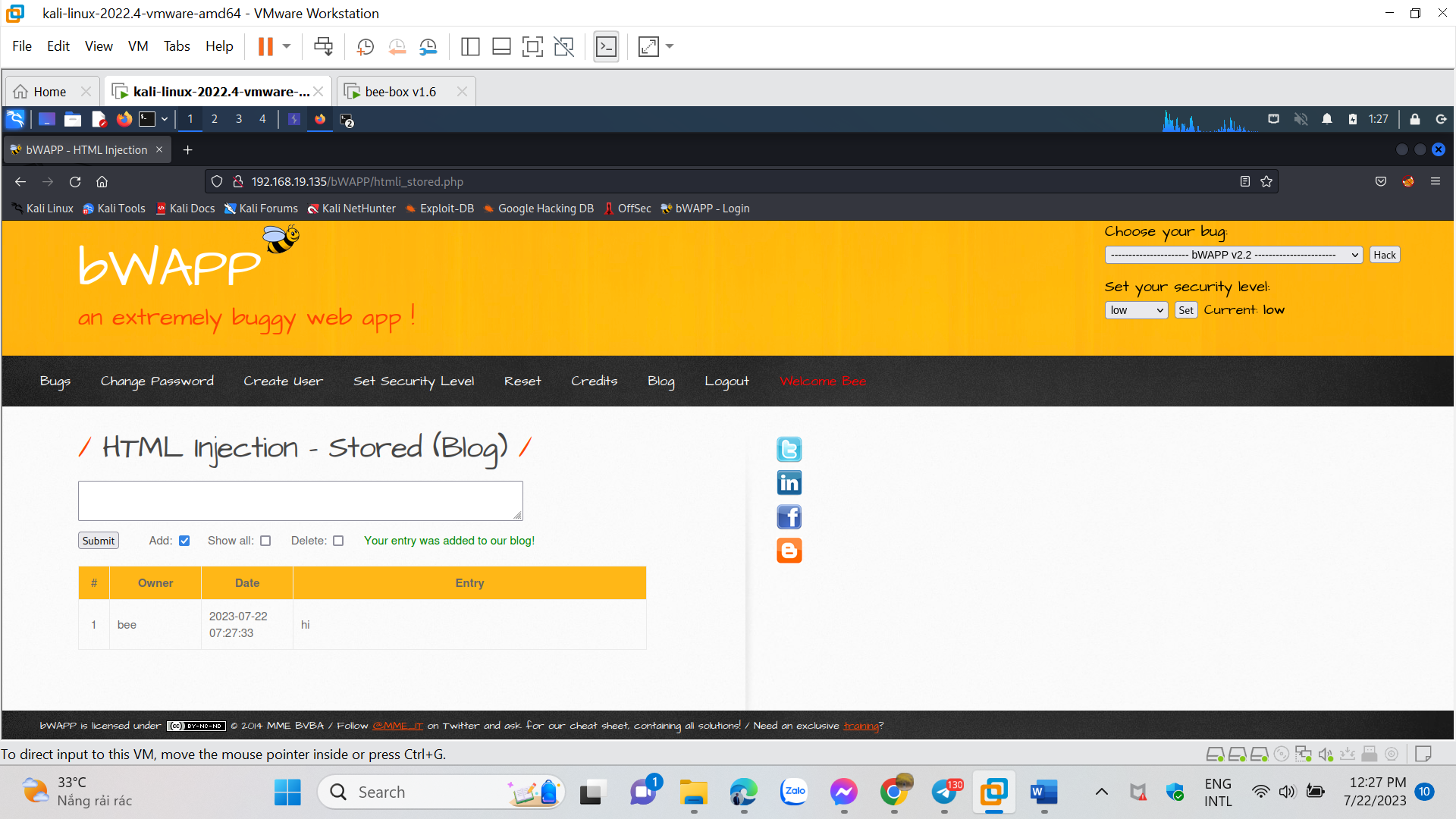
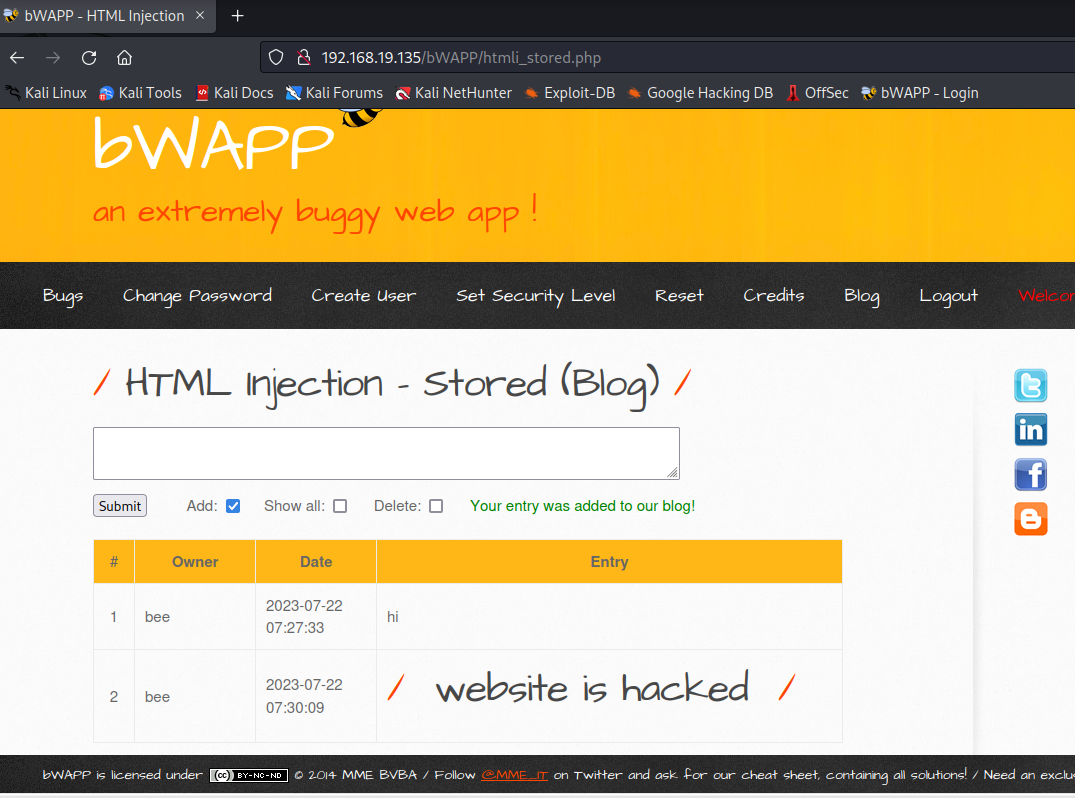
**HTML INJECTION (STORED)**

Giới thiệu lại về Stored HTML Injection, Stored HTML injection xảy ra khi đoạn mã HTML độc hại được lưu trữ vào web server và được thực thi mỗi khi user gọi một tính năng phù hợp. Loại tấn công này thường ảnh hưởng đến nhiều người dung.

Ở bài lab này, ta sẽ khai thác vào 1 trang web có chứa Stored HTML Injection trên Bwapp.

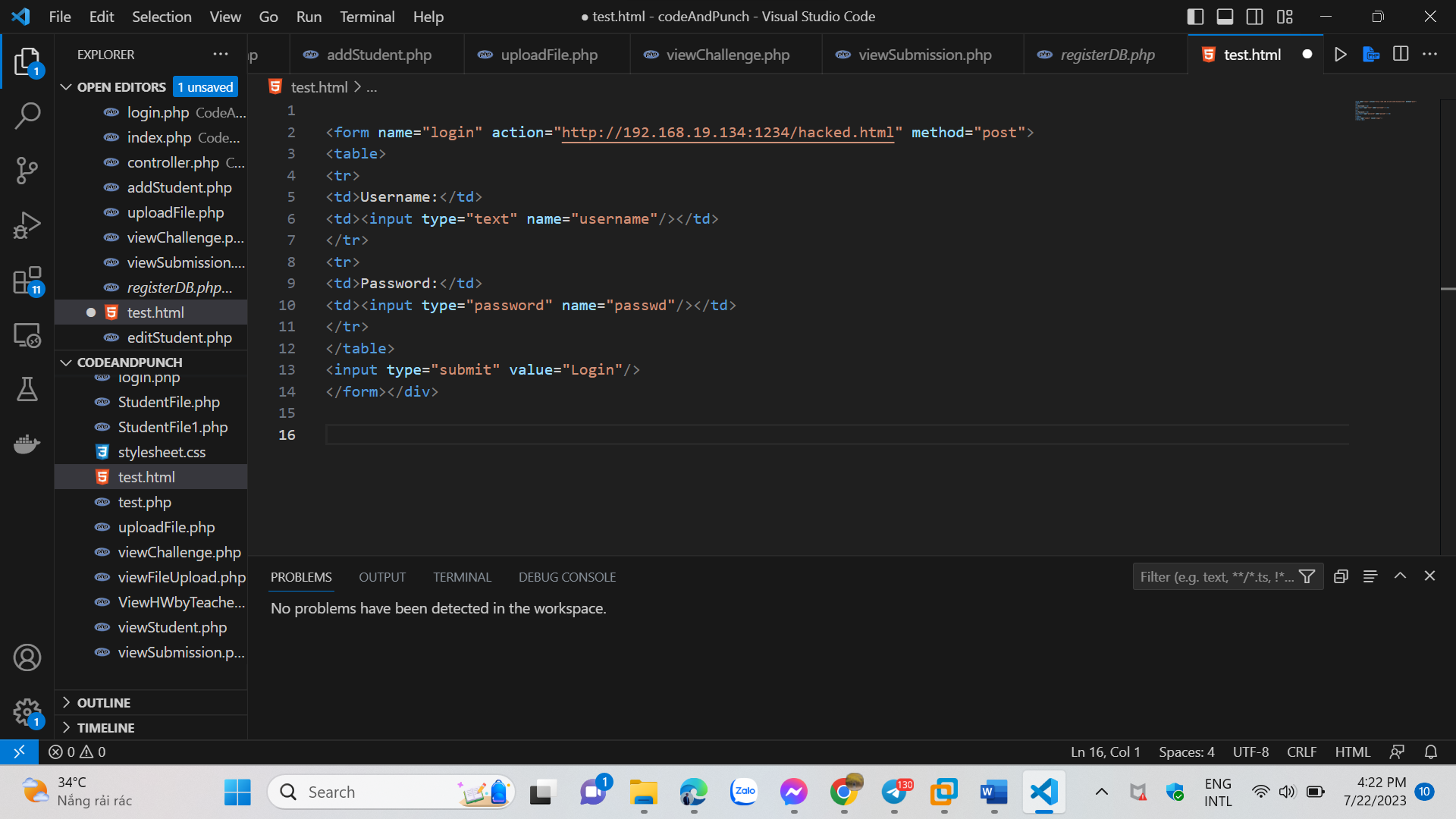


Giao diện trang web. Sau khi nhập dữ liệu ta thấy dữ liệu được lưu trữ vào table ở phía dưới. Ta thử nhập 1 đoạn code html

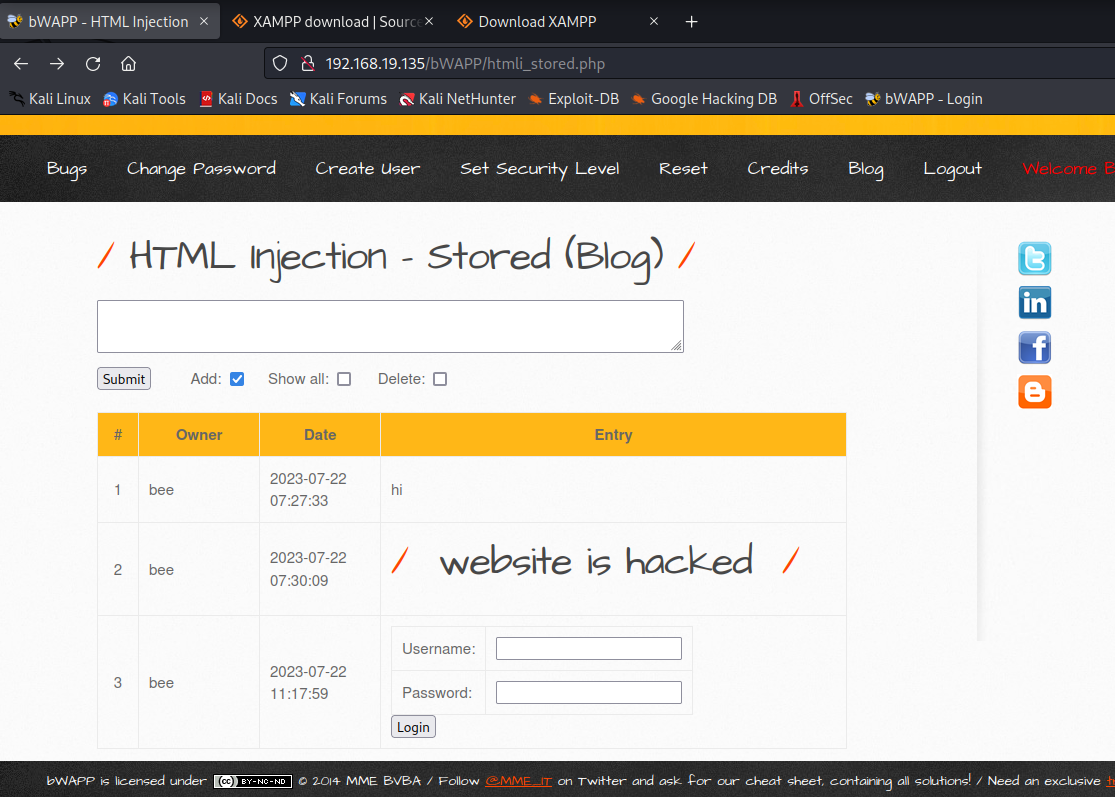


* Kết quả sau khi nhập

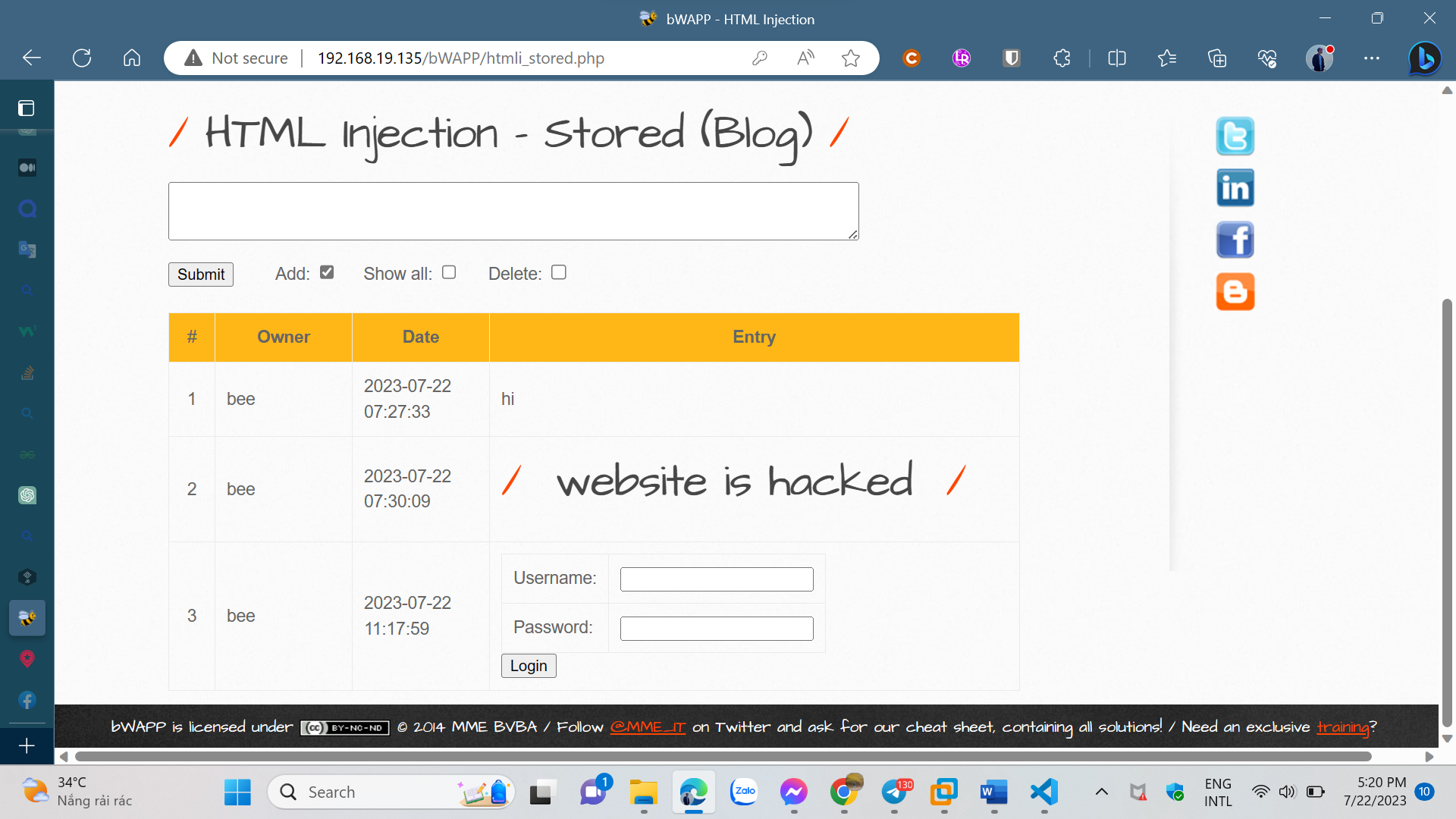
Từ đó, ta sẽ thử chèn 1 đoạn code login form thay vì những code hiển thị trên màn hình thông thường.



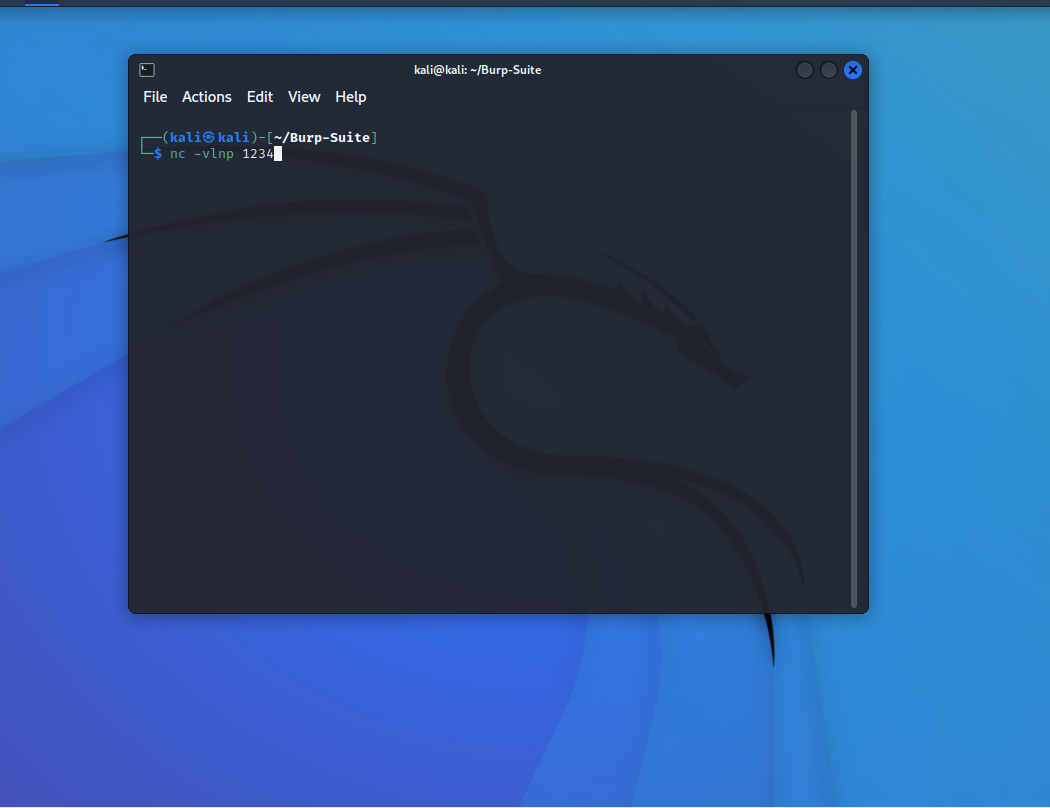
Đây là 1 cuộc tấn công giả mạo đánh lừa người dùng nhập thông tin vào form login, nhưng thực chất form login này được kết nối tới ip của máy chủ attacker. Khi người dùng nhập thông tin sẽ được ghi lại qua hệ thống của attacker. ở hệ thống này, máy attacker là máy ảo kali linux của mình



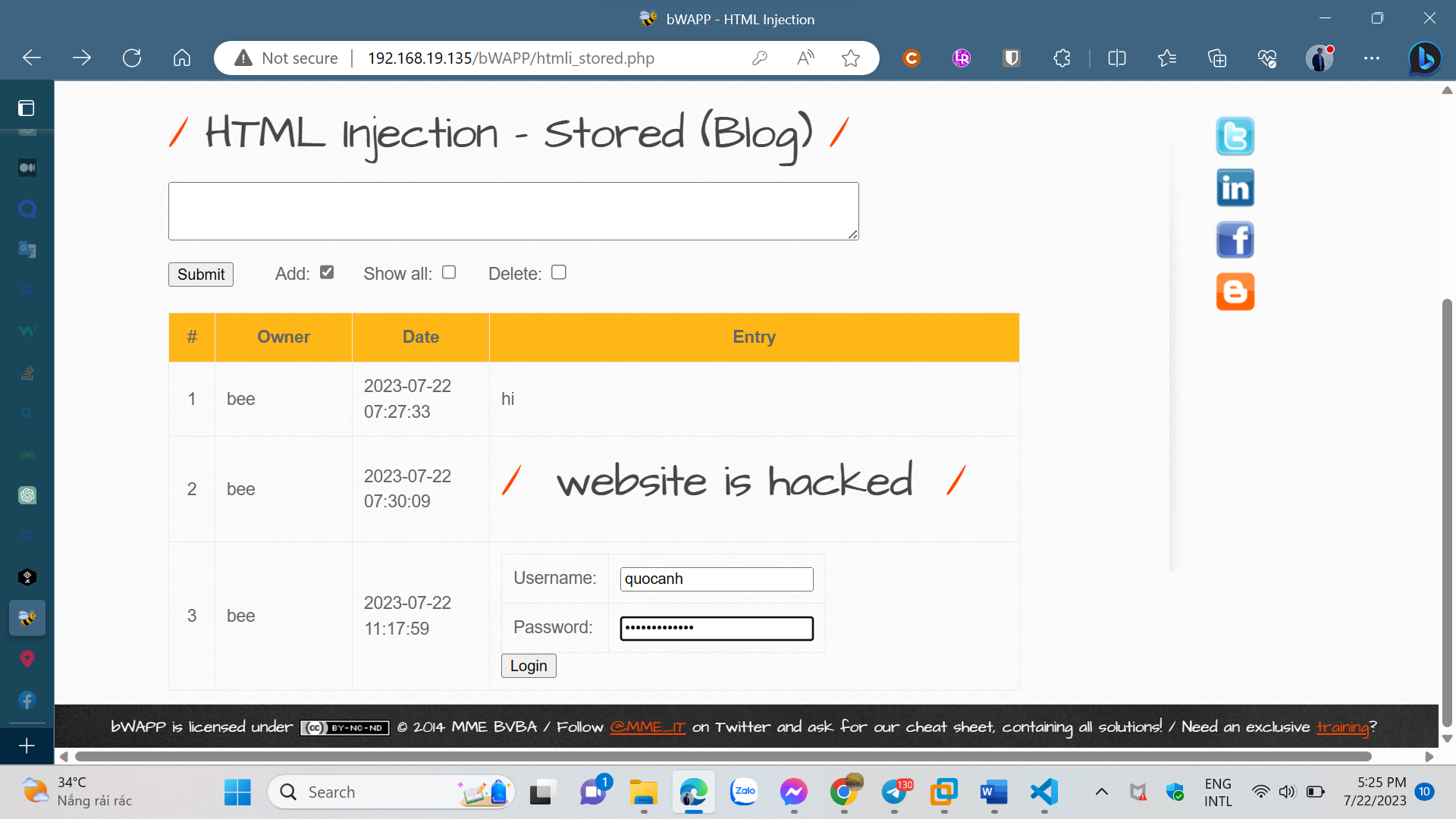
Website sau khi inject malicious code.



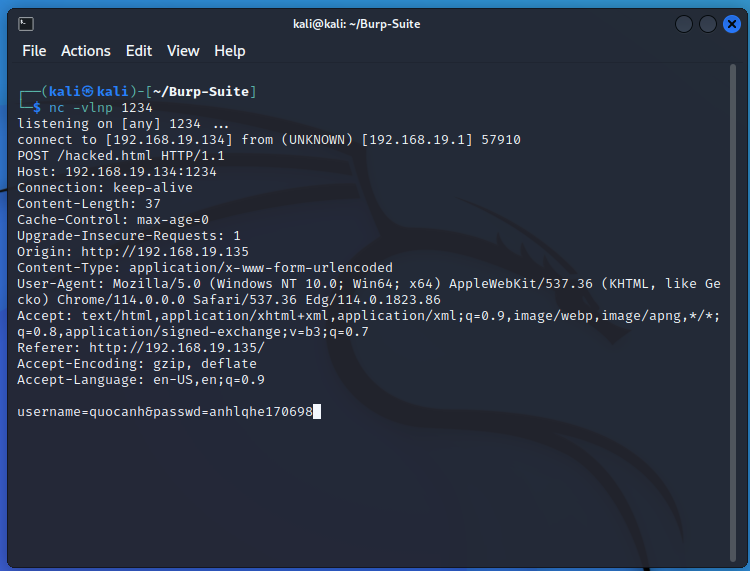
ở đây, mình sẽ vào web thông qua máy thật win 11.



ở phía máy ảo chúng ta sẽ chạy natcat listener ở port 1234



Khi nạn nhân nhập đấy đủ thông tin và ấn submit, web sẽ chuyển hướng sang 1 trang web khác có tên là hacked.html.



Đồng thời, bên phía máy ảo đã ghi lại được thông tin đăng nhập của nạn nhân với

Username: quocanh || password: anhlqhe170698

**Kết luận** : khác với reflected html injection , stored html injection nguy hiểm hơn rất nhiều khi nó lưu trữ những malicous code được tiêm vào trang web bởi hacker.